



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,767	10/22/2001	Mark Lucovsky	13768.198.6	4885

7590

09/26/2005

WORKMAN, NYDEGGER & SEELEY
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/003,767	Applicant(s) LUCOVSKY ET AL.	
	Examiner Jung W. Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 10/01, 7/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

69

DETAILED ACTION

1. Claims 1-36 are pending.

Information Disclosure Statement

2. The items listed on the Information Disclosure Statements filed on October 22, 2001 and July 8, 2002 have been considered.

Specification

3. Claims 30 and 33 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The text as to whether a claim is a proper dependent claim is that it shall include every limitation of the claim from which it depends (35 U.S.C. 112, fourth paragraph) or in other words that it shall not conceivably be infringed by anything which would not also infringe the basic claim. MPEP 608.01(n).III. Regarding claims 30 and 33, they define a computer-readable medium comprising computer-executable instructions for performing the acts recited in the independent method claims 1 and 31 respectively. Hence claims 30 and 33 do not include every limitation of the claims from which they depend.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 30, 33-35 are rejected under 35 U.S.C. 101 because the claims are not limited to tangible embodiments. In view of Applicant's disclosure, specification pg. 11, paragraph 24, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., hardware) and intangible embodiments (e.g., transferred digital data). As such, the claim is not limited to statutory subject matter and is therefore non-statutory.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 2, 4, 24, 26 and 30-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Deinhart et al. USPN 5,911,143 (hereinafter Deinhart).

7. As per claim 1, Deinhart discloses a computer network that includes different types of data structures, a method for authorizing a requesting entity to operate upon data structures in a standard manner, the method comprising:

- a. an act of maintaining a plurality of role templates that define basic access permissions with respect to one or more command methods, wherein at least some of the role templates define access permissions in a manner that is independent of the type of data structure being accessed (fig. 2C, "Role Type 2");
- b. an act of maintaining a plurality of role definitions that define access permissions for specific entities by using one or more of the role templates (fig. 2C, "Job Position 6");
- c. an act of receiving a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity (col. 10:37-40);
- d. an act of identifying a role definition corresponding to the requesting entity (10:39-40); and
- e. an act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity (fig. 7).

8. As per claim 2, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, the act of maintaining a plurality of role definitions that define access permissions for specific entities comprises:

f. an act of the role definition corresponding to the requesting entity using at least one access permission that is specific to the requesting entity, wherein the access permission for the requesting entity are defined by the one or more role templates that are used by the corresponding role definition as well as the access permission that is specific to the requesting entity (figs. 1, 2B and 2C).

9. As per claim 4, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, the request identifies the requesting entity by identifying a user as well as a corresponding application that is making the request, wherein different role definitions may apply depending on both the identification of the user as well as the corresponding application (fig. 2A, "Persons 5" and "Organizational Units 7 & Job Positions 6"; fig. 2C).

10. As per claim 24, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, the data structure represents role list information (fig. 2B).

11. As per claim 26, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, the act of identifying a role definition corresponding to the requesting entity comprises an act of identifying the role definition by searching a database (figs. 2B, 2C and 7).

Art Unit: 2132

12. As per claim 30, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, Deinhart discloses a computer-readable medium comprising computer executable instructions for performing the acts recited in claim 1 (col. 3:5-33).

13. As per claims 31 and 32, Deinhart discloses a computer network that includes different types of data structures, a method for authorizing a requesting entity to operate upon data structures in a standard manner, the method comprising:

- g. an act of maintaining a number of role templates that define basic access permissions with respect to a number of command methods, wherein at least some of the role templates define access permissions in a manner that is independent of the type of data structure being accessed (fig. 2B and 2C, "Role Type 2"; 8:10-31, "relative resource sets");
- h. a step for authorizing a requesting entity using the role templates in a manner that is independent of the type of data structure being accessed (figs. 2A and 2C, col. 7:13);
- i. wherein the step of authorizing comprises the following:
 - i. an act of maintaining a plurality of role definitions that define access permissions for specific entities by using one or more of the role templates (fig. 2C);

- ii. an act of receiving a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity (fig. 2C; 10:39-40);
- iii. An act of identifying a role definition corresponding to the requesting entity (fig. 7); and
- iv. An act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity (fig. 2C and 7).

14. As per claim 33, the rejection of claim 32 under 35 U.S.C. 102(b) is incorporated herein. (supra) In addition, Deinhart discloses a computer-readable medium comprising computer executable instructions for performing the acts recited in claim 31 (col. 3:5-33).

15. As per claims 34 and 35, they are claims corresponding to claims 31-33 and they do not teach or define above the information claimed in claims 31-33. Therefore, claims 34 and 35 are rejected as being anticipated by Deinhart for the same reasons set forth in the rejections of claims 31-33.

16. As per claim 36, Deinhart discloses a computer network that includes different services, applications, and an authorization station, the applications submitting requests to perform operations on different data structures managed by the different services, a

Art Unit: 2132

system for isolating the authorization process from the services so that the services need not independently authorize each request they receive from the number of applications (fig. 2A), the system comprising:

- j. a plurality of services, each service configured to facilitate operations on one or more types of data structures (col. 7:13);
- k. an authorization station configured to receive requests from a number of applications to operate upon data structures managed by any of the number of services, the authorization station configured to perform the following:
 - v. receive a request to perform a target operation upon a target data structure managed by a target service (fig. 7, reference nos. 5, 6 and 41);
 - vi. in a manner that is independent of the data structure desired to be operated upon, determine that the corresponding requesting entity is authorized to perform the target operation on the target data structure (fig. 2C; 8:10-42); and
 - vii. communicate to the target service that the requesting entity is authorized to perform the target operation on the target data structure (8:44-45).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

19. Claims 19-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deinhart.

20. As per claims 19-23 and 25, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) Deinhart discloses the data structure represents objects in a computer system (col. 1:7-18), but Deinhart does not expressly disclose the data structure represents the following: in-box information, calendar information, document information, notification information, content information, or system information. However, it is notoriously well known for these types of information to be placed under access restriction: in-box information is specific to the receiver of the in-box; calendar information lists the personal obligations scheduled for a given date; document information contains a litany of personal documents; notification information is private to

Art Unit: 2132

the notifies; content information relates to all of the above; and system information is restricted to administration privileges. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the data structure to represent any one of in-box information, calendar information, document information, notification information, content information, or system information, since all of these information require access restriction to maintain the privacy of the information as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 19-23 and 25.

21. Claims 3, 5-17 and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deinhart in view of Wong et al. "A role-based access control model for XML repositories" (hereinafter Wong).

22. As per claims 3, 27, 28 and 29, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) Deinhart does not expressly disclose the request includes an identification of credentials used to authenticate the requesting entity, wherein the role definition corresponding to the requesting entity is identified using the credential identification, wherein different role definitions may apply depending on the credentials; wherein the act of identifying a role definition comprises an act of identifying the role definition based on authorized role information provided within the request; wherein the authorized role information includes an identification of a role template; and wherein the authorized role information further includes an identification of at least one refined, local

Art Unit: 2132

scope. Wong discloses the use of XML to define a role-based access control model wherein access is enabled by means of credential information to authenticate the requesting entity, wherein the role definition corresponding to the requesting entity is identified using the credential identification, wherein different role definitions may apply depending on the credentials; wherein the act of identifying a role definition comprises an act of identifying the role definition based on authorized role information provided within the request (pg. 143-144, RBXAC in XML, 'Configuration File'; especially pg. 144, "users::= user_id password"). Further, an authorized role information includes an identification of a role template (pg. 144, "users::= user_id user_info* password RolePointer*"), and the authorized role information further includes an identification of at least one refined, local scope (pg. 144, role tree defines two local scopes: students and staff). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the request to include an identification of credentials used to authenticate the requesting entity, wherein the role definition corresponding to the requesting entity is identified using the credential identification, wherein different role definitions may apply depending on the credentials; wherein the act of identifying a role definition comprises an act of identifying the role definition based on authorized role information provided within the request; wherein the authorized role information includes an identification of a role template; and wherein the authorized role information further includes an identification of at least one refined, local scope; since XML is emerging as the new standard for data representation across a distributed environment, and discretionary access control on XML data based on a role-based access control model

Art Unit: 2132

is highly desirable (Wong, pg. 138, Introduction). The aforementioned cover the limitations of claims 3, 27, 28 and 29.

23. As per claim 5, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) Deinhart does not expressly disclose maintaining a plurality of role templates that define basic access permission comprising an act of maintaining a role map document that contains all of the role templates for a particular service. Wong discloses the use of XML to define a role-based access control model wherein a plurality of role templates is contained in a role map document for a particular service (pg. 143-144, RBXAC in XML, 'Configuration File', <role-tree>). This role map document outlines the various roles as defined in a hierarchy, wherein each role defines a collection of job functions (pg. 144, 1st column). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the act of maintaining a plurality of role templates to comprise an act of maintaining a role map document that contains all of the role templates for a particular service, since XML is emerging as the new standard for data representation across a distributed environment, and discretionary access control on XML data based on a role-based access control model is highly desirable (Wong, pg. 138, Introduction). The aforementioned cover the limitations of claim 5.

Art Unit: 2132

24. As per claim 6, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following:

- l. an act of defining one or more scopes that describe views on a data structure (Wong, pg. 144, the configuration file defines 2 scopes under University people: students and staff); and
- m. an act of defining a role template by associating a method type with one or more scopes (Wong, pg. 144, "role::= ... role*").

25. As per claim 7, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following: an act of maintaining a role map document as a hierarchical data structure (Wong, pg. 144, configuration file).

26. As per claim 8, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following: an act of maintaining a role map document as an XML document (Wong, pg. 144, configuration file).

Art Unit: 2132

27. As per claim 9, the rejection of claim 1 under 35 U.S.C. 102(b) is incorporated herein. (supra) Deinhart does not disclose the act of maintaining a plurality of role definitions comprising an act of maintaining a role list document that contains all of the role definitions for requesting entities that may attempt to access data structures belonging to an identity. Wong discloses the use of XML to define a role-based access control model wherein the plurality of role definitions for requesting entities to access data structures belonging to an identity is contained in a role list document. (pg. 143-144, section "RBXAC in XML", "users::= ... RolePointer*"). This role list document lists the roles each user has a membership (pg. 144, 1st column, "users"). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the act of maintaining a plurality of role definitions comprising an act of maintaining a role list document that contains all of the role definitions for requesting entities that may attempt to access data structures belonging to an identity, since XML is emerging as the new standard for data representation across a distributed environment, and discretionary access control on XML data based on a role-based access control model is highly desirable (Wong, pg. 138, Introduction). The aforementioned cover the limitations of claim 9.

28. As per claim 10, the rejection of claim 9 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role list document comprises the following: an act of defining a role definition by referencing a role template included in a role map document (Wong, pg. 144, "users::= ... RolePointer*").

29. As per claim 11, the rejection of claim 10 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role list document comprises the following: an act of maintaining a role list document as a hierarchical data structure (Wong, pg. 144, configuration file).

30. As per claim 12, the rejection of claim 10 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of maintaining a role list document comprises the following: an act of maintaining a role list document as an XML document (Wong, pg. 144, configuration file).

31. As per claims 13-17, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the act of receiving a request from the requesting entity to perform at least one of the command methods comprises the following: acts of receiving a request from the requesting entity

- viii. to insert a portion into the data structure;
- ix. to delete a portion from the data structure;
- x. to update a portion of the data structure;
- xi. to replace a portion of the data structure; and
- xii. to query a portion of the data structure (Wong, pg. 142, "The RBXAC model", 4th component).

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chandramouli, Ramaswamy "Application of XML Tools for Enterprise-Wide RBAC Implementation Tasks" discloses using XML and it's associated api's to implement enterprise wide RBAC.

Jerbic et al. «Hewlett Packard Position Paper to the Worldwide Web Consortium Workshop on Web Services, April 11th and 12th» discloses problems and solution requirements for implementing authorization and accountability information on XML documents. One of these solution considerations defines mapping names to roles, and mapping roles to authorizations across a plurality of services.

Vuong et al. « Managing security policies in a distributed environment using extensible markup language (XML) » discloses concepts for managing RBAC security policies using XML.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

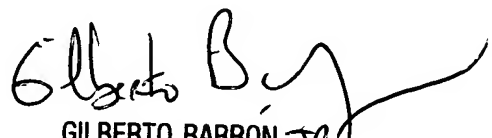
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



September 13, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100